Sony attack shows shifting online security threat

September 4 2014, by Yuri Kageyama

In this June 13, 2013 file photo, attendees play video games on the PlayStation 4 at the Sony booth during the Electronic Entertainment Expo in Los Angeles. The boundary between the online and physical worlds got blurry last week when Sony's PlayStation Network was disabled by an online attack, while an American Airlines passenger jet carrying a Sony executive was diverted due to a bomb threat on Twitter. Experts say that's a wakeup call for a world still coming to grips with cybersecurity: What goes down online can be equally if not more disruptive in the real world. (AP Photo/Jae C. Hong, File)

The boundary between the online and physical worlds got blurry last week when Sony's PlayStation Network was disabled by an online attack, while simultaneously an American Airlines passenger jet carrying a Sony executive was diverted due to a bomb threat on Twitter.

Experts say that's a wakeup call for a world still coming to grips with cybersecurity: What goes down online can be equally if not more disruptive in the real world.

What often surfaces from the Internet's underbelly to make headlines are acts that verge on pranks, and the culprits who get caught are the amateurs, such as a teenager in the Netherlands who tweeted a threat to an airline, saying she was part of al-Qaida and was planning to do "something really big."

But that's just the tip of the iceberg of 24-hour criminal action in cyberspace.

The serious players are after much bigger trophies such as wreaking havoc with defense systems and stealing valuable corporate information. The days of computer mischief to say "I was here," common several years ago, are over.

"Professionals are all in it for the money," said William Saito, an entrepreneur and technology expert who advises the Japanese government and teaches at several universities. "The ones that get caught are usually novices, known in the industry as 'script kiddies,' getting caught for the real-world equivalent of shoplifting."

For every "kiddy," there are 10 professionals, he said.

Japan's Capitol Hill, or Kasumigaseki central government, is targeted in cyberattacks at the rate of one per every six seconds, including viruses,

data leaks and unlawful access, according to the Japanese government.

Public awareness of the threats is low.

"Until it happens to them or someone they know, it is not a concern for them," said Curt Esser, a cyber-security expert who heads Esser Consulting in Wisconsin.

"Hackers and cybercriminals keep coming up with new ways to bypass systems, many unimaginable to comprehend ahead of time," said Esser.

The consequences of a successful infiltration into the networks of companies and institutions could be drastic: disrupting power supplies, sending a stock price plunging, immobilizing traffic or even threatening global security.

In this Aug. 29, 2014 file photo, attendees at the Penny Arcade Expo, a fan-centric celebration of gaming in Seattle, walk past adjoining displays from gaming giants Sony PlayStation and Microsoft's Xbox One. The boundary between the online and physical worlds got blurry last week when Sony's

PlayStation Network was disabled by an online attack, while an American Airlines passenger jet carrying a Sony executive was diverted due to a bomb threat on Twitter. Experts say that's a wakeup call for a world still coming to grips with cybersecurity: What goes down online can be equally if not more disruptive in the real world. (AP Photo/Ted S. Warren, File)

The problems are rarely allowed to escalate to disruptive levels, but that may simply be sheer luck.

"The threat is real, and few nations are adequately prepared," Ian Wallace, a cyber-security expert at Brookings Institution, a Washington D.C.-based nonprofit organization, wrote recently in the Fletcher Forum of World Affairs.

In the Sony Corp. incident, no personal information was stolen. A 2011 attack had compromised the personal data of 77 million user accounts.

Last week, hackers orchestrated a so-called denial-of-service attack, overwhelming the game network with fake visits so that legitimate users couldn't get through. That kind of attack is not very sophisticated and is more a notoriety play.

The American Airlines flight with six crew and 179 passengers was diverted to Phoenix after a Twitter account called Lizard Squad suggested there was a bomb on the plane. It also claimed responsibility for the online attack.

Timothy Ryan, managing director at New York-based Kroll, which investigates hundreds of cybercrime cases a year for corporate clients, said the greed, maliciousness and other motives have not changed, only the tools.

One person stole an algorithm from the company where he worked to try to start his own company, Ryan said.

Another created a technological "crisis," to get attention to his own skills at "solving" it, in an attempt to save his job while framing an innocent co-worker.

"Motivations have not changed. Humans are humans," he said.

Tracking crimes in cyberspace is extremely difficult because the culprits often zip from server to server, using anonymizing services, to disguise their real whereabouts.

In this Monday, Sept. 1, 2014 file photo, Sony Computer Entertainment Japan and Asia (SCEJA) President Atsushi Morita speaks during SCEJA press conference in Tokyo. The boundary between the online and physical worlds got blurry last week when Sony's PlayStation Network was disabled by an online attack, while an American Airlines passenger jet carrying a Sony executive was

diverted due to a bomb threat on Twitter. Experts say that's a wakeup call for a world still coming to grips with cybersecurity: What goes down online can be equally if not more disruptive in the real world. (AP Photo/Eugene Hoshiko, File)

Complicating the investigation further is that sometimes groups are involved, and each participant takes on a stage of a crime, such as credit card fraud, some of them knowing each other only online.

In Japan, the difficulty of tracking the Internet user has led to the arrests of the wrong person, such as a 2012 case of online threats to destroy a shrine and stab its priestesses.

On another front, former National Security Agency contractor Edward Snowden told Wired magazine last month that the NSA had secretly planned a cyberwarfare program, codenamed MonsterMind, that could automatically fire back at cyberattacks from foreign countries without any human involvement.

Cybersecurity firm Mandiant has published detailed research showing that the Chinese military is involved in hacking to steal government, military and corporate information.

Others are activists pushing what they see as a noble cause, such as the U.S. and U.K-based LulzSec hacker collective that grew out of the Anonymous movement and has agitated on behalf of the WikiLeaks online secret-spillers and Occupy Wall Street.

In this Tuesday, Sept. 2, 2014 photo, Japanese ruling party lawmaker Takuya Hirai, who oversees information technology, speaks about cyber crimes at his office in Tokyo. The 2020 Tokyo Olympics are certain to be a target, and that worries Hirai. Preparations must start immediately as hackers may plant a virus now that takes off later like a time bomb. The 2012 London games were targeted, but damage was minimized only because money was spent to guard against the attacks, he said. (AP Photo/Yuri Kageyama)

Japanese ruling party lawmaker Takuya Hirai, who oversees information technology, is pushing for legislation, expected to pass soon, to regulate cybersecurity in Japan, a nation he acknowledged lagged behind the rest of the industrialized world in that area.

The 2020 Tokyo Olympics are certain to be a target, and that worries Hirai. Preparations must start immediately as hackers may plant a virus now that takes off later like a time bomb.

The 2012 London games were targeted, but damage was minimized only because money was spent to guard against the attacks, he said.

"The skills to hack and to defend against hacking are actually the same. It's the question of whether that person will be Darth Vader or a Jedi," Hirai said.